Intelligence Community Staff
Washington, D.C. 20505

IC-83-2211

24 May 1983

31 MAY 1983

NOTE FOR: DCI
VIA: DDCI

SUBJECT: Recommendations on the Leak Problem

The attached memorandum presents our ideas and some recommendations on the leak problem. It is the product of two things: (1) three separate meetings with senior staff personnel, and (2) the carefully considered thoughts over a long period of time of the Security Committee. I think it is pretty comprehensive, and some of the ideas have a lot of merit. Unfortunately, the memorandum is also rather long and not well suited for a quick review. My purpose in sending it along as is--and encouraging you to take the time to go through it--is to give you a timely input as you consider remedial action.

We are going to continue to pursue the subject and will advise you of any additional thoughts. And, of course, we are ready to respond to any requirements that you may have for us to develop policies and procedures for the Community.

25X1

Attachment

DCI EXEC REG

13.				
14.				
15.				

FORM 610 USE PREVIOUS EDITIONS 1-79

SECRET

S-110

SECRET

Director
Intelligence Community Staff
Washington, D.C. 20505

ICS-0802-83

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence

25X1 FROM: [redacted]
Director, Intelligence Community Staff

SUBJECT: Unauthorized Disclosures of Classified Information (U)

1. Senior members of the Intelligence Community Staff have met to consider responses to your call for proposals to counter the unauthorized disclosures of classified intelligence which are increasing in number and severity. The recommendations of the group are in five basic categories -- education, legislation, investigations, media interface and information control. This memorandum discusses proposals in each of these categories.

2. Education - There appears to be a lack of appreciation of the consequences of the unauthorized revelation of classified intelligence information, both to the national security and to the individual making the disclosure. Each recipient of Sensitive Compartmented Information (SCI) is indoctrinated on the potential damage to the national security of such revelations, as well as the penalties prescribed in Title 18, Sections 793 through 798. Nevertheless, incidents continue which indicate that these elements of risk are not being taken seriously. Recipients of classified intelligence must be convinced that its unlawful revelation is reprehensible, and that individuals who take it upon themselves to decide when the system may be ignored place the national security and themselves in jeopardy.

3. In wartime, the population recognizes the need to keep military secrets. The concept that "loose lips sink ships" is well accepted. We need a campaign, beginning with the President, to convince all concerned that classified information must be protected if we are to avoid national disaster. A vigorous Presidential charge to the Cabinet and the Executive Office of the President, relayed through channels to all levels, is an essential element of this campaign.

4. Awareness of the importance of security to intelligence must be extended to the Congress. The whole-hearted cooperation of both legislators and staff members is indispensable. Not only is Legislative Branch support needed to safeguard the material provided to the Congress, but also to put teeth into the anti-leak effort.

through legislation.

CL BY SIGNER

5. To make this effort credible, documents must be classified properly and concern about disclosures should be limited to those affecting national security.

6. A one-time effort to sensitize the government and the public to the disastrous consequences of illegal disclosures, even one kicked off by the President, has a limited half-life. There must be a planned follow-up. In addition to the obvious reindoctrination efforts, consideration should be given to an ongoing program of damage-oriented "lessons learned" presentations. These are envisioned as timely, specific, succinct and technically competent videotape shows detailing the nature of the unauthorized disclosure and the specific losses suffered as a result. They would be shown to audiences cleared for the compromised information as a means of reinforcing the need for strong security.

7. Because of the general derision with which the media regard government efforts to stop leaks and because the generic term "leak" is associated with disclosures that are politically embarrassing, It may be advisable to avoid that term and speak only of "unauthorized disclosures of classified information."

8. Legislation - The existing espionage laws were drafted to protect U.S. secrets from foreign agents. They did not contemplate the hemorrhaging of classified data that has followed the media explosion. The divulgence of classified information to the Russians by way of Jack Anderson's column, for example, is a relatively new phenomenon. Even though the intentions of the leaker may be to nobly inform the public of facts he thinks should be known, the results are the same as directly transmitting the information to the KGB.

9. Attached is a copy of the proposed bill to prohibit certain unauthorized disclosures of classified information. Formulated on the basis of the Willard Report, it is an excellent vehicle for closing the loophole that allows individuals to ignore classifications and make their own decisions about what must or must not be kept secret. Passage of such a bill would make it clear that both the legislative and executive branches are serious about preserving our ability to keep our national security secrets. It would then remain for the judiciary to show the same resolve.

10. The chances of passing the unauthorized disclosures bill are directly related to the Congress's perception of how responsibly the Executive Branch uses its classification powers. As noted above, the effort to educate government employees (and the public, to the extent possible) on the need for effective secrecy must also include the Congress and legislative staff personnel. The means of reaching this objective are the same for both branches of government -- graphic demonstrations that unauthorized disclosures are costly in terms of money, national defense, intelligence capabilities, and sometimes, human lives.

11. Legislation also is needed to make the unauthorized possession of classified material a crime. It is illogical for the U.S. Government to be

unable to bring charges against, or at least sue to recover classified material from, Jack Anderson, who makes a mockery of classification, or from
25X1 Aviation Week and Space Technology
25X1 [redacted] If the U.S. would take action against an ordinary citizen, it should act with the same vigor against journalists who damage the national security. The Attorney General and the General Counsels of the Intelligence Community should begin a crash program to draft a legislative proposal and to review the possibilities of action even without a new law.

12. Whether or not the effort to pass new legislation is successful, it is vital that Congress be included in any awareness-raising program. A secondary objective would be to raise the security standards of the congressional staffs. Many staffers have access to more sensitive information than some CIA or NSA personnel, who are polygraphed as well as backgrounded, and are subject to periodic reprocessing. Congressional staffers are not steeped in the discipline of security as are the intelligence professionals, and would almost certainly benefit from a greater appreciation for the need for secrecy.

13. Finally, the problem of reinforcing the responsibilities of formerly cleared recipients of classified information to continue to maintain secrecy requires attention. A periodic reminder by mail might be considered, but except for CIA and NSA, it could be difficult to identify those who should receive them. In the future, the archival file of the Community-wide, Computer-assisted Compartmented Control (4C) System, which will contain the identities of individuals formerly approved for access to SCI, should assist with this problem. Meanwhile, the message needs to be spread that our "old boys" can do a lot of harm by talking too much. Cleared persons still employed in government must be reminded frequently and forcefully that those who have retired, or taken jobs in the industrial sector, may not legally receive classified information unless they are specifically cleared for it.

14. Investigations - The investigation of unauthorized disclosures has rarely proven successful over the years. The broad dissemination required of intelligence reporting, the lack of an effectual investigative program throughout the government, an apparent tolerant attitude toward those who make illicit disclosures, and the absence of a legislative basis for action have made for a highly frustrating situation. NSDD-84 offers hope for greater success in the future, but there is much to be done.

15. Although leak investigations are searches for needles in haystacks, occasionally good investigative work will produce results. Unfortunately, unauthorized disclosures to the media are consensual acts between two parties, neither of whom is likely to admit participation, and one of whom enjoys a special degree of privilege under the First Amendment. Legislation will help, but there can't be a trial until a defendant is identified. The abysmal track record of leak investigations to date dictates that the Federal Bureau of Investigation is the only agency with any chance of success. Fragmented, single-agency efforts simply do not work. Nor does the proposal to form interagency units to investigate unauthorized disclosures offer any reasonable hope for improvement.

16. Even the FBI will require some help -- the full cooperation of other agencies, the legislation discussed earlier, and guidelines that permit the use of as full a range of investigative tools as possible. The Attorney General and the Director of the FBI should be instructed by the President to provide the most permissive guidelines possible, consistent with the protection of civil liberties, for FBI investigations of unauthorized disclosures of classified information. In addition, appropriate manpower allocations to the FBI should be made to ensure a vigorous effort to solve unauthorized disclosures. Without this, the Bureau cannot be expected to neglect other important investigations to undertake tasks that offer a low probability of success and almost certain criticism in the press.

17. Because of the nature of unauthorized disclosures, the likelihood of developing conclusive evidence is low. In fact, the investigative tool most likely to succeed is the polygraph, if conventional investigation can narrow the number of suspects sufficiently to employ it. If a suspect confesses as a result of polygraph interview the case is solved. If, however, in the face of clear-cut polygraphic evidence of deception he continues to deny culpability, the problem of acceptability of polygraph evidenee arises.

18. While prosecution on the basis of polygraph charts is extremely unlikely to succeed, the government could revoke the individual's clearances or access approvals on that basis. This would effectively neutralize future disclosures by that individual, but could result in a lawsuit to regain the approvals. The Justice Department and Intelligence Community legal counsels should be tasked to research the grounds upon which such a suit could be defended and the likelihood of success.

19. Action based primarily upon polygraph results is certain to bring strong media criticism. The polygraph process is little understood and the press has fostered this misunderstanding by pressing the theme that the instrument itself is unreliable. Consideration should be given to preparing an educational program to be used first with senior officials of the Executive Branch and with legislators. It should demonstrate that the effectiveness of the process doesn't depend totally upon the machine, but is a technique to aid a skilled interrogator. If a convincing effort can be mounted, it could be brought to the public and even to the news media. If the Intelligence Community can't provide objective, rational evidence that the polygraph process is reliable, the entire effort to combat unauthorized disclosures may be in serious trouble.

20. Press Interface - NSDD-84 mandates policies to govern contacts between media representatives and agency personnel, leaving implementation to the individual agencies. The effort to eradicate unauthorized disclosures would be assisted greatly by the adoption of uniform rules for all agencies.

21. The discussion of government information, especially sensitive intelligence, by a government employee is not a private, personal matter. There seems no reason why the government cannot require the reporting of all contacts with the news media, during or outside of duty hours, in which

government business is discussed. Failure to follow such a rule could be made subject to administrative sanctions of varying severity. Data on such contacts could be computerized, by names of government employees, names of media representatives, subjects of discussions and dates of contacts, providing a means of determining a great deal of information that could take inordinate amounts of investigative effort. It wouldn't tell who made unauthorized disclosures, but it would provide a means of determining who might have had the means and the opportunity, and possibly even the motive to have done so.

22. It would be ideal, from the standpoint of security, to abolish backgrounders. Recognizing that this isn't going to happen, there should be firm control of background briefings to the press. There must be clear-cut guidelines on who may authorize and present backgrounders. Every such briefing should be attended by a security or public affairs officer who knows what is sensitive about the topic being discussed and is capable of offering guidance to the briefer. A record should be kept of briefings by names of participants and authorizing officials, dates and topics, preferably in a computerized mode. Presenters of background briefings should be required to prepare summaries of what was presented. These should be cross-referenced to the automated index of background briefings. The documentation of this information and its retrievability will not only serve as an invaluable investigative resource, but its existence will promote prudence in the presentation of backgrounders and in other dealings with the press.

23. Even if all these proposals were adopted, there would be individuals who would continue to divulge classified information to the press. But they would find themselves operating at considerably greater risk. Simple failure to comply with the reporting requirements would be cause for administrative sanctions, and it would become easier to detect such failures by having a reliable record of compliance. It is likely that associations between government personnel and media representatives are known to at least some associates of both, and the possibility of being reported by a concerned colleague would be enhanced by the revised rules. An effective education program about leaks should have the salutary effect of highlighting to their associates those who may deal with the media without observing the reporting requirements. If those who comply are sufficiently convinced of the need for regulation of press contacts, they may be inclined to "blow the whistle." It would then be necessary for the government to demonstrate the seriousness of its intent by taking administrative action against the nonreporting individuals, regardless of their positions.

24. The matter of "authorized" or "official" leaks needs close attention. If the appropriate official determines it is in the national interest to release for publication information that was classified until that point, there should be a means of recording that fact. Such a record would appropriately be kept somewhere in the Executive Office of the President. This record could provide a means of avoiding the expenditure of resources to investigate such disclosures as "leaks."

25. Finally, the revolving door practice of appointing national media personalities as top level government press officers should be carefully reexamined. Such appointments must face the incumbents with conflicts of interest and severely ambivalent feelings, both during and after their federal service. It may be unrealistic to expect them to deny their colleagues information which they feel is unjustifiably classified and to expect them to forget, and never use, information they received officially.

26. Information Control - Some people believe there are enough information control policies, procedures and regulations on the books to bring the government to a complete halt if they were strictly applied. While this view may have some merit, it should not serve as an excuse for not trying to secure our sensitive information. The concept that security is everybody's business must not be given lip service and then cast aside.

27. Except for the need for developing a strong, national information control program for the emerging electronic information systems, it is unlikely that more document control regulations are needed or practicable. What is needed is for everyone to be educated in the existing policies and procedures and to make a renewed effort to comply. While everyone claims to know the regulations, it is likely that few could pass a comprehensive test on information security and control.

28. Steps to improve information control would include detailed comparison of practices with policies; the reeducation of all personnel in information security, and a motivational program to enhance awareness of the consequences of improper handling of sensitive intelligence. Better information control is needed, but it must come from motivated people. More regulations are not the answer.

29. Summary - Unauthorized public disclosures of classified information in the news media are damaging to the national security. Our defense against them must come from within, from those who are cleared for access to, and who have signed agreements to protect, classified information. It is clear that some of these people, for reasons of their own, have not kept their word. It also appears that neither the overall level of concern about this situation nor the government's capability for remedial action is up to the job.

30. To encourage wholehearted support of our efforts to protect classified information, we must convince those who have agreed to keep the secrets that they have a moral and legal obligation to keep that convenant. The rules on SCI are simple and clear. It is inconceivable that anyone who gives such information to uncleared individuals is unaware of what he is doing. Therefore, such persons must be unconvinced of the seriousness of the security program.

31. A massive reeducation program for all legitimate recipients of classified information is the first step in attempting to achieve the necessary change in attitude.

32. A policy and resource commitment to the solution of at least the most flagrant cases of unauthorized disclosure is also needed. This means the devotion of sufficient FBI assets to investigations and an all-out effort to obtain passage of unauthorized disclosure laws.

33. A severe tightening of policies concerning relationships of cleared individuals with media representatives is essential. To be meaningful, this must include strict guidelines, reporting procedures, information retrieval capabilities, and impartial administrative penalities for noncompliance.

34. Renewed awareness of information control policies and procedures and their importance to the national security is needed. If classified documents can be turned over to the media or other unauthorized persons without being noticed, the system isn't working. It must be made clear that "the system" really is the people who operate it.

35. If you wish elaboration or action on any of the above items, appropriate elements of the Intelligence Community Staff are prepared to assist in any way possible.

25X1

Attachment:
Draft unauthorized disclosures bill

All paragraphs of the text
are classified SECRET

SUBJECT: Unauthorized Disclosures of Classified Information

Distribution:
Orig - Addressee w/att
1 - DDCI w/att
1 - ER w/att
1 - D/OS/CIA w/att
1 - D/ICS w/att
1 - C/SECOM w/att
1 - C/UDIS w/att
1 - ICS Registry w/att

In the course of Administration development of the Fiscal Year 1984 Intelligence Authorization Bill, the Intelligence Commmunity obtained from the Office of Management and Budget clearance of provisions which would establish criminal penalties for certain unauthorized disclosures of classified information. The provisions were based on the report of the Interagency Group on Unauthorized Disclosure of Classified Information chaired by Deputy Assistant Attorney General (Civil Division) Richard K. Willard and were coordinated with Deputy Assistant Attorney General (Criminal Division) Mark Richard, as well as with the Office of the Secretary of Defense/Legislative Affairs.

For a number of reasons, including the issuance of NSDD 84 just before the Authorization Bill was forwarded to the Hill, and in deference to the intelligence committees' preference for handling the Intelligence Authorization in as unobtrusive a manner as possible, the unauthorized disclosures provision ultimately was not transmitted as part of the Authorization Bill. The proposal has now been configured as a separate bill, and it has been prepared for transmission at an opportune moment as a tripartite initiative from the DCI, the Secretary of Defense and the Attorney General.

A BILL

To protect against injury to the national defense and foreign relations of the United States by prohibiting certain unauthorized disclosures of classified information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That Chapter 37 of title 18, United States Code, is amended by adding at the beginning thereof the following new section:

"§ 791. Unauthorized Disclosures

(a) Whoever, being an officer or employee of the United States or a person with authorized access to classified information, willfully discloses, or attempts to disclose, any classified information to a person who is not an officer or employee of the United States and who does not have authorized access to it, shall be fined not more than $10,000, or imprisoned not more than three years, or both.

(b) Whoever, being an officer or employee of the United States, willfully discloses any classified information to an officer or employee of the United States with the intent that such officer or employee disclose the information, directly or indirectly, to a person who is not an officer or employee of the United States and who does not have authorized access to it, shall be fined not more than $10,000, or imprisoned not more than three years, or both.

(c) As used in this section--

(i) the term "classified information" means information or material designated and clearly marked or represented, pursuant to the provisions of a statute or Executive order, as requiring protection against unauthorized disclosure for reasons of national security;

(ii) the term "disclose" or "discloses" means to communicate, furnish, deliver, transfer, impart, provide, publish, convey, or otherwise make available;

(iii) the term "authorized access" means having authority, right, or permission to receive information or material within the scope of authorized intelligence activities or pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency who is empowered to classify information, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which governs handling of classified information by the respective House of Congress.

(d) Nothing in this section shall be construed to establish criminal liability for disclosure of classified information in accordance with applicable law to:

(i) any court of the United States, or judge or justice thereof; or

(ii) the Senate or House of Representatives, or any committee, subcommittee or joint committee thereof.".

SEC. 2. The table of contents of Chapter 37 of title 18, United States Code, is amended to include the following caption:

"791. Unauthorized Disclosures".

SECTION BY SECTION EXPLANATION

Section 1 of the Bill amends chapter 37 of title 18, United States Code, to include a section 791 prohibiting certain unauthorized disclosures of classified information. Section 2 of the Bill makes the corresponding changes in the table of contents for chapter 37 of title 18.

Proposed section 791 of title 18, United States Code, provides criminal penalties for willful unauthorized disclosures of classified information by federal employees and others who have authorized access to classified information, such as government contractors. With the narrow exceptions of unauthorized disclosures of atomic energy Restricted Data, communications intelligence/cryptography information, and the identities of covert agents, willful unauthorized disclosures of classified information by those entrusted with it by the government are not per se offenses under existing federal criminal statutes.

Subsection (a) of § 791 prohibits willful disclosure or attempted disclosure of classified information, by a federal civilian or military officer or employee or other person with authorized access to such information, to any person who is neither a federal civilian or military officer or employee nor a person with authorized access to such information. The subsection provides criminal penalties of not more than three years imprisonment or a $10,000 fine, or both, for such willful unauthorized disclosure of classified information.

Subsection (b) of § 791 prohibits willful disclosure of classified information by a federal civilian or military officer or employee to another such officer or employee with the intent that the latter disclose the information, directly or indirectly such as through a chain of intermediaries, to a person who is neither a federal civilian or military officer or employee nor a person with authorized access to the classified information. The criminal penalties for such an offense are identical to those provided for the offense defined in subsection (a).

Subsection (c) of § 791 defines key terms employed in subsections (a) and (b) in defining the offenses of willful unauthorized disclosure. Paragraph (i) defines "classified information" to consist of information or material designated as requiring protection against unauthorized disclosure for reasons of national security pursuant to a statute or Executive order. Paragraph (ii) defines the term "disclose" or "discloses" to include all forms of disclosure enumerated in the existing provisions of 18 U.S.C. §§ 793-798 and 50 U.S.C. § 426. Paragraph (iii) defines the term "authorized access" to include authority or permission to receive information within the scope of authorized intelligence activities or pursuant to the routine security clearance processes of the Executive

branch, orders of the courts of the United States, or rules of either House of Congress. Authorized intelligence activities are those conducted pursuant to statute or Executive order, such as the current Executive Order 12333 governing United States intelligence activities.

Subsection (d) of § 791 assures that no criminal liability will attach under subsections (a) or (b) to otherwise lawful disclosure of classified information to the Congress or the courts.

SECRET

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-111

18 May 1983

MEMORANDUM FOR: Director, Intelligence Community Staff

25X1 FROM: [redacted]
Chairman

SUBJECT: Leaks

1. Attached is a copy of the paper on leaks I sent forward in November 1982. It recommends that the FBI be tasked to investigate particularly damaging leaks (paragraph 7); discusses the need for legislation to criminalize the unauthorized disclosure of classified information by federal employees (paragraph 13); comments on the efficacy of the use of the polygraph (paragraph 12); and the reporting of media contacts and regulation of "official leaks" (paragraph 11). The creation of a data base on leaks does not offer short-term relief, but could have benefits, over time.

2. The Justice Department ought to take vigorous action to recover classified information in the possession of the media as a result of unauthorized disclosures. Justice also should explore the possibility of prosecution of illegal publishers of COMINT, the divulgence of which, under Section 798 of Title 18, is a crime whether or not the recipient is a foreign government. The risk of making media martyrs militates against attempting to prosecute publishers of classified data, but the Justice Department ought to at least evaluate the implications of moving against those media elements who

25X1 [redacted]

3. More indoctrination of government personnel on the damaging effects of leaks is certainly in order, especially for those not accustomed to security as a way of life. The videotape produced by SECOM as an introducton to security for newly-appointed government officials heavily emphasizes the need for caution in dealing with the press. It might be suitable for showing at your staff meeting. The Defense Intelligence Agency also has a videotape on leaks which could help with the indoctrination problem.

ORIG CL BY SIGNER
DECL OADR

4. The discussion of leaks at your Thursday morning meeting should prove interesting. Perhaps a new approach to the problem will surface. SECOM will continue to seek ways to deal with unauthorized disclosures, but without substantial redirection of effort throughout the Community, the existing conditions are likely to continue to prevail.

25X1

Attachment

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-357
1 November 1982

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence
Director, Intelligence Community Staff

25X1 FROM: [redacted]
Chairman

SUBJECT: Unauthorized Disclosures of Classified Information

1. Action Requested: DCI support for three recommendations intended to provide at least modest action toward determining the sources of unauthorized disclosures of classified information. A fourth recommendation encourages continued DCI support of the Willard Report.

2. Background: The problem of leaks--disclosures of classified intelligence to the news media or other unauthorized persons--is the oldest, most frustrating, and most unmanageable problem facing the DCI Security Committee. The SECOM first came together in 1959 to seek a way to deal with leaks. On untold occasions since then, senior officials of the government have decried the apparent impossibility of keeping a secret in Washington.

3. The number of studies of how to stop leaks, or to identify and penalize leakers, is exceeded only by the number of leaks that have occurred. The situation grows worse because of the ambivalence about leaks in the highest levels of government. On one hand, leaks are despicable because they foreclose the options of the policy makers and/or jeopardize the national security. On the other hand, a well-placed leak can be used to enhance greatly the image of the leaker, his programs and policies or to seriously discredit his adversaries or their programs and policies. The leak is a two-edged sword, not easily surrendered by those who feel the need to influence public opinion.

4. As Winston Churchill and others have observed, "The Ship of State is the only vessel that leaks at the top." It is generally believed that most disclosures of classified data are made by persons who (a) are knowledgeable, (b) have trusted contacts in the media, and (c) have motivation, selfish or political. Few, if any, minor bureaucrats possess all of these characteristics. Even if a "leaker" is found, he may have sufficient support from influential friends to avoid being penalized.

5. The procedure for investigating leaks of sensitive intelligence information has been unchanged for at least two decades. First, a determination is made that sensitive information has been disclosed. The document from which the compromised information came is then identified and the authorized dissemination of the document is determined. In the typical case, the dissemination is found to be well into the hundreds, with recipients in several departments and agencies, both within and outside the Intelligence Community. With everyone who saw the hundreds of documents a potential suspect, and with the inability of agencies to investigate outside their own organizations, the situation is normally declared hopeless and the investigation is dropped. In some cases, a few people will be asked whether they were the source of the leak. They promptly deny responsibility, and the matter is closed. If anything has been proven in a quarter of a century of trying, it is that this procedure does not work.

6. It has been suggested that the successful investigation of only a few cases, resulting in well-publicized and appropriately severe penalties, could drastically change the attitude of the federal bureaucracy toward leaks. Many have thought that having the Federal Bureau of Investigation investigate leaks would be an ideal solution to the problem. This is hampered by the Justice Department's requirement that the agency requesting the investigation answer a series of questions, one of which is whether the leaked information can be declassified to permit prosecution. This places the complaining organization in the position of either declassifying the information and insuring its confirmation and further dissemination, or declining to declassify, insuring that the FBI will not undertake the investigation. Even under ideal conditions, the FBI would not have the resources to investigate each leak that occurs. Therefore, a process for selecting the leaks worthy of investigation is needed.

7. A leak rarely is a one-agency phenomenon. Typically, information is gathered by one agency or more, analyzed and turned into finished intelligence by one or more others, and then disseminated to the entire Intelligence Community (and sometimes to agencies outside the IC). Any effective leak investigation must cross agency lines and do so quickly. Delays or failures resulting from lack of resources, lack of interest, or simple inefficiency in any agency or department can be fatal to the investigative effort. Yet it is the nature of bureaucracy that no department or agency head will willingly allow investigators from another agency to conduct inquiries on his turf. The vigor with which internal investigations are pursued may be tempered by fear of the embarrassment that would result from finding a "leaker" within one's own agency or department, or by the attitude that the problem is really someone else's. Any solution to the problem requires an investigative organization whose jurisdiction throughout the government is recognized and accepted. Only the FBI meets this criterion.

8. The tools available for investigating leaks are inadequate. Not only are there far too few investigators, whose charters are hopelessly narrow, but

there is no useful data base to aid probers. Funds have been sought without success to assemble a Community-wide computerized register capable of electronically sorting leaks by topic, publication, organizations having access, identity of reporter, dates of publication, etc. The possibility of constructing a mosaic which could point toward a leaker would be greatly enhanced by such a program. Nor is there any capability in the Community for a long-term analytical study of leaks. Instead, leak investigation is a reflexive activity, stimulated by the publication of sensitive data, and resulting each time in the stylized "kabuki dance" response described earlier in paragraph 5.

9. Perhaps just as debilitating is the inability to use certain investigative techniques without risking the wrath of the fourth estate. Polygraph testing can be done with relative impunity only by CIA and NSA because their employees are routinely tested. Wiretapping, a perfectly respectable investigative technique when done with the necessary legal sanctions, is out of the question politically. Physical surveillance is about as bad. The net effect is a contest in which the advantages are all on the side of the leaker, while the investigators must bear disabling handicaps.

10. The real issue is whether the Government is serious about leaks. Willingness to pay the price for stopping them has not existed heretofore. And a steep price it is, indeed. It would mean government officials would have to give up trying to manipulate the media. (Maybe the price is not so high in this regard, as it seems the media always come out ahead.) It would also mean that government officials would have to endure considerable abuse from the media, which would try to make a First Amendment issue of any serious effort to curtail leaks. The original text of NSDD-19 was directly on target, but the Washington Post reported its issuance before it could be disseminated fully. Its immediate rescission reflected the serious concern of the Administration with the dire consequences of a policy that inevitably would be labeled by the media an attempt to abridge the First Amendment rights of Federal employees. It is clear that there is no way to shut down the torrent of leaks in a manner that will please the media.

11. Among measures which should be considered to try to give the investigators an even break with the leakers is a firm policy prohibiting Executive Branch personnel from giving information to the media without attribution. They should be required to insist upon being identified as the source of the information, and anyone providing information without attribution would be in violation of this policy and subject to penalties. As insurance against appearing to violate this rule, officials should be encouraged to report all contacts with the media to a designated component of their own departments or agencies. For those situations where a leak is believed to be in the national interest, a focal point to register and clear leaks could be established in the Executive Office of the President or the National Security Council. This would separate the so-called "official leaks" from the inadvertent or deliberate disclosures committed by individuals on their own.

12. It is ironic that one of the most vigorous, and possibly most successful, leak investigations in recent memory concerned the revelation of UNCLASSIFIED deliberations of the Defense Resources Board in spring 1982. All those attending the board meeting were polygraphed, and the culprit apparently identified. External factors caused his punishment to be commuted. But the case proved that unauthorized disclosure cases can be solved if resources are brought to bear and sound investigative tools are used.

13. Legislation is needed to criminalize unauthorized disclosures of classified intelligence by Federal employees even when a foreign government is not the recipient, but its enactment is extremely unlikely. No one has been successfully prosecuted under the Espionage Statutes for an unauthorized disclosure, as distinguished from providing information to a foreign power. An Executive Branch policy requiring reporting of all media contacts by persons with access to classified information seems remote, given the fate of the original NSDD-19. The only adjustment in the leak investigation procedure that seems practicable is to provide the FBI with the marching orders and the manpower to investigate the publication of classified information. The goal of the investigation need not be prosecution. It could be the enhancement of the national security by determining how the leak occurred and taking corrective measures. If the investigation results in the identification of the Federal employee responsible for the leak, then the possibility of prosecution or administrative sanctions can be considered. Meanwhile, steps can be taken to shore up any weaknesses in security policy or practice uncovered by the investigation.

14. The SECOM has requested, most recently in the FY 1984 budget submission, funding for a Community-wide leak data base and for a study of the origins, nature and consequences of leaks. The lack of success of this initiative may reflect the true attitude of the Community--that leaks are worth bemoaning but not worth the expenditure of funds. It is essential that we try to quantify and qualify the leak problem. This can be done only by assembling a body of information upon which to base evaluations of leaks, including how many times specific information has been published, the most likely sources, and what has been lost as a result of leaks. It is not my purpose to flog a dead horse, but I strongly feel that further delay of an empirical approach to leak evaluation and investigation dooms us to continue repeating the mistakes of the past.

15. The SECOM, at its recent seminar, voted to try to assemble a task force to review a limited area of intelligence activity to determine the extent of damage resulting from leaks. This effort will be handicapped by the lack of a data base but will rely upon its narrow focus to seek appropriate conclusions. If the effort is successful, it will prove that a data base is vital to a broad review of the nature of the leak phenomenon and to any progress toward a solution. The SECOM also voted unanimously to recommend that the DCI offer to the Attorney General the services of the Unauthorized Disclosures Investigations Subcommittee to assist in evaluating and prioritizing leaks for investigation by the FBI.

16. A word of caution. The FBI is not eagerly seeking this task--it is thankless, places the organization's public relations at risk, and has no guarantee of success. It offers, however, the possibility of breaking the impasse we reached long ago. The Bureau is not likely to accept the job without additional manpower, and even then acceptance will be reluctant. Nor does providing funds for the creation of a leak data base assure us of putting a stop to leaks. But the data base is a tool without which we cannot hope to understand, let alone solve, the leak problem. Unfortunately, some of those who complain loudest about leaks seem least willing to share their resources to combat them. It is time for us to put up or shut up.

17. The Willard Report, prepared by a committee headed by the Department of Justice, contains many useful recommendations to help remedy the unauthorized disclosure problem. The report is a wide-ranging document, however, and is still being mulled over by the NSC Staff. This paper recommends action which can be undertaken in the near future and which can be accomplished without legislation or massive funding.

18. Recommendation: That the DCI:

a. Sponsor, in consultation with the Director, FBI and the Attorney General, an initiative calling on the FBI to investigate selected leaks whether or not prosecution is expected to ensue, and providing additional manpower to offset FBI personnel requirements to conduct leak investigations. Approximately 12 positions should provide a respectable level of effort. The DCI should be prepared to provide advice on the selection of leaks for investigation in order to keep the FBI workload within manageable limits.

b. Reprogram FY 1983 NFIB funds ($250,000 and 3 positions),and plan for similar resources in FY 84 and beyond, to provide the Security Committee the means to establish and maintain a computerized, Community-wide, leak data base for use in analyzing leaks for patterns or trends.

c. Reprogram FY 1983 NFIP funds ($125,000) to provide the Security Committee resources needed to contract an analytical study of the long-term effects and characteristics of leaks.

d. Continue vigorous support of the findings and recommendations of the Willard Report.

25X1

SUBJECT: Unauthorized Disclosures of Classified Information

APPROVED: Recommendation A

Director of Central Intelligence Date

APPROVED: Recommendation B

Director of Central Intelligence Date

APPROVED: Recommendation C

Director of Central Intelligence Date

APPROVED: Recommendation D

Director of Central Intelligence Date

Distribution:
Orig - Return C/SECOM
1 - DCI
1 - DDCI
1 - ER
1 - D/ICS
1 - D/OCC/ICS
1 - ICS Registry